Commonwealth of Virginia Cyber Security Commission

DRAFT Report, July 7, 2015

"Threats and Opportunities"

Please note: This is a preliminary document that is currently under revision.

Table of Contents

Executive Summary

With daily reports of cyber attacks and data breaches, the protection of computers and information systems has come to seen as an uphill battle against an increasingly sophisticated and relentless adversary. But in spite of the resources devoted to new technologies and policies to protect information systems, cyber security need not be focused only on defensive strategies and capabilities. As an enabling technology, cyber security creates market opportunities and can deliver significant benefits – new, innovative technologies, demand for research and education and a growing, creative, engaged workforce – that contribute to building the New Virginia Economy.

Virginia is well positioned to take advantage of the opportunities presented by cyber security. Already, over 65,000 of its citizens work in cyber security-related fields, and the demand for trained workers is expected to grow by 25 percent through 2020. The Commonwealth's university system stands ready to deliver that workforce with over a dozen degree and certification programs in computer and information systems security. And as home to many security-focused federal agencies – and the contractors, entrepreneurs and researchers that support them – the Commonwealth has built a robust technology ecosystem that lays the foundation for a similar leadership role in cyber security.

To ensure that the Commonwealth can truly capitalize on the opportunities presented by cyber security challenges, Governor Terry McAuliffe formed the Virginia Cyber Security Commission in June 2014 to protect information systems infrastructure and data statewide, bolster business investment and foster cyber security education and awareness. In just the first year, the Commission's five work groups conducted research, consulted with cyber security experts in government, industry and academia and held Town Hall meetings with citizens across the state.

This report represents the results of that research, revealing the challenges and opportunities cyber security presents for Virginia in five general areas: economic development, education and workforce, cyber-crime awareness, infrastructure and network protection and public awareness. The Commission's five work groups then made the following recommendations based on insights gained through their activities.

Economic Development

Challenge: Advance economic development opportunities in industries where Virginia already has expertise that intersects with cyber security, specifically advanced manufacturing, advanced automobile automation and unmanned systems.

Recommendations: Build integrated economic development strategies with representatives of the cyber security and advanced manufacturing industries that promote workforce development, create funding opportunities for technologies at the intersection of manufacturing and cyber security and support entrepreneurial investment in those technologies. Investigate low-cost tech options for law enforcement and citizens to analyze cyber vulnerabilities in vehicles. Work with federal partners to streamline access to unmanned systems expertise to support new business development, and establish a university center of excellence to cultivate the technologies and work force pipeline to advance a secure unmanned systems industry.

Education and Workforce

Challenge: Build cyber security-focused science, technology, engineering and math (STEM) programs at all educational levels to develop a skilled workforce pipeline that can support the Commonwealth's growing cyber security industry.

Recommendations: Foster successful two-year cyber security certificate programs and help colleges and universities more quickly develop accredited information assurance degree programs. Increase the number of cyber credentials attained in the Commonwealth. Expand the reach of community colleges and local universities by sharing faculty and resources, and encourage cyber security education in K-12 schools.

Cyber Crime Awareness

Challenge: Ensure that the Virginia's laws and capabilities are current with latest technologies and in step with practices in other states and the federal government to better protect the Commonwealth, its businesses and citizens.

Recommendations: Make it easier to prosecute criminal activity by setting a lower standard of intent for computer trespass crimes and by designating violations of the Virginia Computer Crimes Act as RICO predicate offenses. Establish stricter penalties for computer crimes, especially those targeting government or 'protected' computers and critical infrastructure systems. Request additional personnel for the Virginia State Police High Tech Crimes Division, and leverage universities' facilities and students to address skyrocketing demand for cyber forensics.

Commonwealth's Cyber Infrastructure and Network Protection

Challenge: Identify the vulnerabilities in the networks, data and technology processes in the Commonwealth – not just those supporting the state agencies but also those of local governments, businesses and citizens across Virginia.

Recommendations: Minimize cyber security vulnerabilities in Commonwealth enterprise IT systems and strengthen protection of privacy data. Implement an identity and access management program that standardizes technology and policy across state agencies and simplifies citizen interaction with the Virginia's online services. Increase cyber security education and training for IT staff. Create a Joint Cyber Security Operations Center to gather and disseminate cyber-specific threat and vulnerability information among local, state, federal and private sector partners and programs. Leverage resources of the Virginia National Guard and expand cyber security staffing of the Virginia Fusion Center.

Public Awareness

Challenge: Provide concise, accurate and experience-appropriate information on cyber security best practices for municipalities, business and citizens.

Recommendations: Build a Cyber Information Exchange and Reporting Portal to collect and distribute relevant cyber security information and alerts to specific constituencies.

Call to Action

High-profile cyber attacks on Sony, Target, Anthem Health – and the recent compromise of millions of federal workers' personally identifiable information from Office of Personnel Management systems – have sounded a call to action throughout the nation.

Government data breaches have obvious consequences; they can affect national and regional security, put citizens at risk, aid criminals and provide anti-government groups with information they can use for an attack. Less obvious is that because today's economy depends on stable, safe and resilient physical and cyber resources, any damage to data or infrastructure can have a negative effect on economic vitality. The stakes in protecting the public's data and the nation's information systems continue to mount in the face of increasingly sophisticated and relentless attacks. And governments must respond by boosting defenses of computer systems, ensuring sufficient numbers of workers trained in cyber security, fostering a climate that encourages cyber security business development and providing citizens with the information they need to defend themselves – all while the technology and threats change daily.

Yet cyber security need not be a defense-only game. Great opportunities exist in changing times. New technologies present risks to existing systems, certainly, but they also create first-to-market opportunities with the accompanying economic benefits – more jobs, a creative, engaged workforce and a thriving economy.

Recognizing both the threats and opportunities presented by cyber security, Governor Terry McAuliffe has acted quickly and decisively to protect the Commonwealth's assets and to promote and nurture its already vibrant cyber security ecosystem. A month after taking office, Governor McAuliffe announced that Virginia would adopt the elements of the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity into its own risk framework to help identify and communicate cyber security risks.

Then, with Executive Order 8, signed on February 25, 2014, Governor McAuliffe created the "Cyber Virginia" initiative and chartered the Virginia Cyber Security Commission to "mitigate risks and safeguard the highest level of security for government infrastructure networks, foster cyber security education and awareness, incorporate innovative and best practices to protect data statewide, bolster business investment with public-private partnerships and proactively enhance Virginia's national standing as one of the preeminent leaders in the cyber security arena." Formed in June 2014, the Commission, composed of six cabinet members and 11 Virginia citizens with exceptional cyber security background and expertise, engaged support from public and private sector subject matter experts, met frequently and worked to deliver on the preliminary objectives laid out in the executive order.

The Commission's work was almost immediately apparent in bolstering the Commonwealth's cyber security posture.

Several bills were introduced and passed in the 2014-2015 General Assembly legislative session that strengthen Virginia's laws to protect citizens and business from cyber crime, to increase penalties for crimes affecting government or critical infrastructure systems and to make it easier for the state to prosecute cyber criminals:

- SB919 and HB1946 (Wexton/McClellan) help protect Virginia children from online exploitation and allow law enforcement to effectively investigate crimes involving child pornography, child exploitation and human trafficking by sealing administrative subpoenas for electronic communications and social networking data.

- SB1307 (Wexton) clarifies language for search warrants surrounding the seizure and examination of computers, networks and other electronic devices.

- SB1109 and SB1129 expand FOIA exemptions for sensitive information regarding cyber security threats and vulnerabilities.

In 2015, building on the work of the Virginia Cyber Security Commission, Governor McAuliffe took executive action and worked with members of the General Assembly to strengthen the Commonwealth's cyber security posture against threats and leverage its technology-rich infrastructure to build more economic opportunities for the citizens and businesses.

- NIST Cyber Security Framework. Virginia was the first state to adopt the National Institute of Standards and Technology (NIST) framework to enhance the systematic process for identifying, assessing, prioritizing, and communicating cyber security risks.(February 12, 2014).

- SB1121 (Barker) makes agency executives responsible for securing the electronic data held by their departments and complying with the Commonwealth's IT security and risk management program (March 17, 2015).

- SB814/HB1562 (Watkins/Rust) creates the Identity Management Standards Advisory Council to recommend technical and data standards for authentication in digital and online transactions (March 23, 2015).

- The Virginia Information Sharing and Analysis Organization is established, the first state-level information exchange to share critical cyber security threat information across levels of government and industry sectors (April 20, 2015).

- Executive Directive 5 directs Commonwealth agencies that accept payment cards from citizens to have advanced card-security features in place by the end of the year, making Virginia the first state to mandate the enhanced protections (May 5, 2015).

- A public-private working group is formed to address the potential for cyber attacks on automobiles and explore the economic development opportunities related to this specialized cyber security field (May 15, 2015).

- Executive Order 43 launches the Unmanned Systems Commission to bring public and private sector experts together to advance Virginia's leadership position in unmanned systems technology and build new business opportunities (June 12, 2015).

These accomplishments help lay the foundation for Virginia to capitalize on the rapidly growing worldwide demand for the technology research, personnel and capabilities needed to effectively combat cyber threats.

As Governor McAuliffe focuses on developing the full potential of the Virginia cyber ecosystem as a key element of his New Virginia Economy initiatives, the Commission and its five topic-specific work groups have been conducting surveys and research, meeting with citizens and consulting with industry and university technology experts in order to strengthen the Commonwealth's cyber security – not just protecting the assets of the state and its citizens against threats – but also positioning industry and workforce to make Virginia the best place for cyber security research, jobs and business opportunities.

Commission Recommendations 2014-2015

The Virginia Cyber Security Commission was formed to identify ways in which the public and private sector can work together to expand Virginia's economic footprint in cyber security technology and protect the Commonwealth from cyber threats. It was also tasked to explore opportunities to advance education in key science, technology, engineering and math (STEM) sectors that will prepare Virginia students for jobs in industries of the 21st century and ensure a cyber security workforce pipeline.

The Commission's policy and technology experts were divided into five work groups that investigated the key foundational elements of a vibrant cyber security ecosystem:

- Economic Development
- Education and Workforce
- Cyber Crime Awareness
- Cyber Infrastructure and Commonwealth Network Protection
- Public Awareness

After extensive research and analysis, the work groups each made specific recommendations on protecting the Commonwealth's information system assets and fueling cyber security-based economic opportunities across Virginia. Those recommendations are detailed below.

Economic Development

The Economic Development Work Group researched three areas of potential economic growth in which Virginia can rapidly take a leadership position: cyber security solutions for advanced manufacturing systems, advanced automation in automobiles and unmanned aerial vehicles. The Economic Development Work Group spun-off three private-public groups to address possible initiatives in each of the targeted areas.

Cyber Security and Advanced Manufacturing
The following initial recommendations were developed to take advantage of Virginia's leadership in cyber security and advanced manufacturing.

Build a cross-industry strategy. Existing manufacturing and cyber security associations should establish a new integrated working group to develop strategies that will ensure the highest level of security in automated manufacturing. Issues to be addressed include cyber security practices, security certifications for advanced manufacturing companies, threat data sharing, workshops on new cyber security technologies and methodologies for joint cyber security technology evaluations, conducted at a laboratory facility such as the Commonwealth Center for Advanced Manufacturing.

Support workforce development. Professional education opportunities should be made available to help managers, regulators and engineers develop new skills related to security of cyber-physical systems. The 4VA University consortium (University of Virginia, Virginia Tech, James Madison University and George Mason University) should establish a professional education program at the University of Virginia that would grant a certificate in cyber security for physical systems. The program could be ready to start in fall 2015.

Consider cross-sector research funding. The Commonwealth should consider co-funding competitive integrated research between cybersecurity and manufacturing companies and universities for new products and services at the intersection of cyber security and advanced manufacturing.

Encourage new company formation. MACH 37, a Virginia economic development initiative engaged in the formation of new cyber security companies, should augment its existing program by considering security opportunities in the advanced manufacturing sector.

Cyber Security for Advanced Automation for Automobiles

As a result of recommendations made by the Virginia Cyber Security Commission, Governor McAuliffe in May 2015 formed a public-private working group to research cyber security in automobiles. This action not only addresses a high-visibility need but also positions Virginia as a leader in cyber-physical systems research for automobiles. Initial proposals from that group include:

Identify low-cost technology that can be developed to assist law enforcement officers and investigators in determining if/when a vehicle or other mechanized equipment has become the target of a cyber attack.

Develop strategies for Virginia citizens and public safety personnel to identify and prevent cyber security threats targeting vehicles and other consumer devices.

Analyze police car vulnerabilities to cyber attacks and create a cyber security scoring system for vehicles similar to what the Virginia-based Insurance Institute for Highway Safety does for crash worthiness.

Cyber Security for Unmanned and Autonomous Aerial Vehicles

Building on the goals of the Unmanned Systems Commission to bring public and private sector experts together to make recommendations on how to make Virginia the national leader in unmanned systems by ensuring that such systems are secure from cyber attacks, the work group recommends the following:

Leverage existing resources such as the National Institute of Standards and Technology, Mid-Atlantic Aviation Partnership and NASA Wallops to develop the cyber security capabilities for unmanned systems that can help create a new industry in Virginia.

Establish a university-based unmanned vehicle cyber security Center of Excellence to support the workforce and technology development needed for this emerging area.

Education and Workforce

In order to fuel economic opportunity and secure Commonwealth information systems and critical infrastructure, greater numbers of qualified cyber security personnel must be in the education and workforce pipelines. Enhanced cyber education and skills training at all levels (K-12 to graduate work) are key enablers for this future workforce.

Although Virginia's university system holds a leadership position in developing professionals with the wide variety of cyber security certificate, degree and professional programs, education efforts must be broader to generate the range of professionals needed. The Education and Workforce Work Group recommends:

Share faculty and facilities. Smaller schools and community colleges should collaborate with larger nearby universities to physically or virtually share resources (especially cyber educators) and establish articulation agreements that ensure qualified community college students have guaranteed access to four-year schools to complete their degree. Fairfax County STEM, Northern Virginia Community College and George Mason University provide an excellent example of a successful articulation pipeline.

Promote two-year programs. Many cyber security positions do not require a four-year degree; in fact, industry leaders interviewed by the work group preferred candidates from two-year accredited cyber security programs because they know the candidate has been trained on specific systems and practices and can make immediate contributions.

Speed program development. Accelerating the pace of accrediting cyber programs in small to mid-sized universities and community colleges will help generate more cyber professionals more quickly.

Certify cyber security educators. Because of the importance of teachers in inspiring students' career choices, the work group requested and received initial seed funding to certify eight to10 K-12 teachers in cyber security education. James Madison University will conduct a program this summer with participation from industry, and the work group will review the results of the program and develop further recommendations for 2015-2016.

Cyber Crime Awareness

The Cyber Crime Work Group reviewed existing statutes governing crimes in cyberspace (see Appendix D for a summary of pending cyber crime legislation). As a result of the group's research, it recommended legislation to support law enforcement in its fight against cybercrime and to protect the public by preventing the release of information that would jeopardize the safety or the security of citizens, facilities and information systems. That legislation included:

SB919/HB1946 (Wexton/McClellan), which seal administrative subpoenas for electronic communications and social networking data.

SB1307 (Wexton), which clarifies language for search warrants surrounding the seizure and examination of computers, networks and other electronic devices.

SB1109/SB1129 (Stuart), which secure FOIA exemptions for sensitive information regarding cyber security threats and vulnerabilities.

As crimes move from the physical world into cyberspace, the work group focused its research on ensuring that Virginia's laws address the latest technologies and are in line with statutes in other states. The group's key recommendations for conducting more effective cyber security investigations and bringing successful prosecutions include:

Allow authentication of Internet content via affidavit. During criminal prosecutions, Virginia Code currently requires all parties to call an Internet Service Provider's custodian of records as a witness to attest to the authenticity of a record of electronic communications. The work group recommends Virginia Code § 19.2-70.3 be amended to allow for the authentication of records by the ISP through the submission of an affidavit, which would alleviate an unnecessary burden on the prosecutor and the ISP authenticating the Internet content.

Set a lower standard of intent for computer trespass crimes. Current law requires that the government prove that computer or network intrusions were committed with "malicious intent," an inordinately high burden to meet. The work group recommends Virginia Code § 18.2-152.4 be amended to set a lower standard of intent to match more current

standards found around the country. This change will better protect businesses' and citizen's personal computers and information.

Establish stricter penalties for computer crimes. Penalties for computer crimes in Virginia are light compared to those of other states and the federal code, which carries felony-level penalties for cyber crimes and cyber security incidents. Rather than treating serious acts of cybercrime as minor violations, the work group recommends that computer crime penalties be reviewed and strengthened to bring them in line with more modern computer crime statutes, indicating the seriousness with which Virginia handles such offenses.

Define and increase associated penalties for crimes targeting government or 'protected' computers and critical infrastructure systems. As recent hacks of the Office of Personnel Management and the IRS have shown, government agencies are at risk of cyber attack as are the systems controlling the nation's critical infrastructure. However, there are no additional penalties under current law for unauthorized access to these systems. The work group recommends that Virginia follow the framework established within the Computer Crimes Act which levies stronger penalties for attacks against government computers and critical infrastructure systems.

Designate violations of the Computer Crimes Act as RICO predicate offenses. Under current law, penalties under the Racketeer Influenced and Corrupt Organization (RICO) Act do not apply to computer crimes even though anecdotal evidence from law enforcement investigations reveals that most major, organized computer crimes are committed across state lines (and even international borders) and typically involve many individuals committing various acts along the criminal chain – the standard definition of a RICO predicate offense. The work group recommends Virginia amend its RICO statute to include crimes covered by the Virginia Computer Crimes Act so as to strengthen penalties against organized crime operating in cyberspace.

Request additional personnel for the Virginia State Police, High Tech Crimes Division (HTCD). The Virginia State Police conducts primary cyber security investigations and supports the Commonwealth's 340 law enforcement agencies, committing its scarce, specially trained staff to federal, state and local investigations. As computer crimes increase in number and complexity, current employees are overwhelmed. Compounded by personnel shortages, resource constraints force many cybercrimes to go unaddressed. The work group recommends hiring additional HTCD staff to deal with these increasing challenges.

Leverage universities to address demand for cyber forensics. Given a limited supply and high demand for cyber forensic analysis expertise, the Virginia State Police HTCD is unable to keep pace with cases requiring cyber forensics, which is becoming increasingly complex because of encryption, mobile devices and cloud computing. The work group recommends leveraging university resources – students and cyber-security and cyber-forensics laboratories – to address HTCD's needs. Using students for some cyber forensic analysis will not only allow HTCD personnel to focus on key cases but also provide invaluable hands-on experience for students looking to enter the field. Furthermore, university laboratories should be made available and used by HTCD and other law enforcement agencies to update and refresh staff cyber forensics skills.

Cyber Infrastructure and Commonwealth Network Protection

The Cyber Infrastructure and Commonwealth Network Protection Work Group identified areas for improvement within the state's information technology systems and processes as well as in those maintained by municipalities, critical

infrastructure operators, small to mid-sized businesses and citizens. The work group based its recommendations on discussions with experts as well as the following activities:

- A survey of the overall cyber security posture of all Virginia agencies. The survey responses have been provided to Virginia Commonwealth University for analysis, development of key findings and initial recommendations.

- Assessment the cyber capabilities of the Virginia National Guard and its ability to provide support for evaluating and enhancing cyber readiness of Virginia municipalities.

- Review of the cyber security processes and procedures being used to protect personally identifiable information (PII) at five Virginia agencies holding large amounts of citizen data.

While the work group expects additional recommendations after the final analyses of the surveys of agency systems and PII protection processes are complete, the initial recommendations generated from the work group activities include:

Establish a Joint Cyber Security Operations Center (JCSOC). While the Virginia Information Technologies Agency (VITA) is charged with incident response and cyber monitoring for Commonwealth agencies and has the authority to provide outreach and assistance to higher educational institutions and independent organizations, there is no organization to deliver those services to Virginia's critical infrastructure providers nor any mechanism for the Commonwealth to ascertain the threats its industries and municipalities face. The JCSOC would to serve as the hub for gathering and disseminating cyber-specific threat and vulnerability information among local, state, federal and private sector partners, providing a common operating picture that fosters the coordination critical to cyber threat prevention and response. In the event of a cyber incident, the JCSOC should be leveraged by the Virginia Emergency Operations Center to provide oversight and resources for a coordinated incident response.

Establish an identity and access management (IAM) program. In order to increase the security of agency-specific applications, the work group recommends that an IAM program be created and that a task force, co-led by the VITA and the Department of General Services, be established to determine a strategy for implementing standard, uniform IAM policies and technology solutions across the Commonwealth's information systems. A standard IAM solution would not only improve efficiency of Commonwealth's systems, but it would also advance efforts to create a single sign-on for citizens to access online services across agencies. A single agency that has experience and a vested interest in identity and access management should be charged with establishing and managing the IAM program.

Strengthen protection of privacy data. To better protect citizens' PII in Commonwealth systems, the work group recommends an agency-by-agency inventory of PII in order to establish a statewide privacy program and a privacy framework for agency data. That program should identify PII best practices, data standards and access requirements as well as processes for conducting breach notification.

Minimize cyber security vulnerabilities in Commonwealth IT systems. To bolster efforts to more completely secure Virginia's computer systems, the work group recommends a review of agency IT security audit programs to ensure all systems are in compliance with Commonwealth security policies and standards. Technology and policy frameworks should be built that mitigate risks for agency IT systems, with specific attention to the supervisory control and data acquisition (SCADA) systems governing critical infrastructure in small and medium-sized business. The work group also advocates aggressively pursuing practices, technologies and polices to protect the Commonwealth enterprise email service, with special focus on minimizing the impact of phishing attacks.

Increase cyber security education and planning. To better prepare agency IT leaders for cyber security challenges, the work group proposes analyzing the feasibility of cyber certification for chief information officers, chief information

security officers as well as centralized security awareness training for Commonwealth employees, with advanced training for security personnel and IT leaders. Additionally, incident response procedures and scenarios that outline specific actions for agencies, VITA and executive team members in the event of a cyber incident should be prepared.

Leverage the Virginia National Guard to provide cyber assessment support to Virginia's municipalities. To address the gap in cyber security capabilities facing many localities, the Virginia National Guard expertise and resources can be leveraged by the Commonwealth to conduct vulnerability assessments of municipal networks and state agency websites.

Expand Virginia Fusion Center's cyber security capabilities. The Virginia Fusion Center works with federal, state and local partners to improve the Commonwealth's preparedness against terrorist attacks and to deter criminal activity. To support the Fusion Center's abilities to provide expertise in cyber security-related initiatives, three cyber analyst positions should be added.

Public Awareness

Over the last year, the Public Awareness Work Group held Town Hall meetings and participated in public events throughout the Commonwealth, reaching more than 500 citizens to explain the objectives of the Virginia Cyber Security Commission, provide cyber insight from subject matter experts and, most important, solicit feedback on attendees' cyber security concerns.

Based on feedback received during the outreach events, the Public Awareness Work Group found that counties, municipalities, small to mid-sized businesses and citizens need a reliable source of clear, concise and understandable cyber threat information, including best practices and processes for requesting cyber security remediation assistance as well as a way to report suspected cyber incidents.

While there are many information exchanges for federal and state cyber security agencies and large businesses (especially those operating critical infrastructure), the same opportunities do not exist at the regional and local levels. Often, cities and counties often cannot afford the cyber security-trained personnel to access threat sharing and remediation resources. Those municipalities with cyber security staff are often challenged to convey the complexity and critical importance of addressing and remediating cyber threats to their leadership.

To address these issues the work group recommends:

Cyber Information Exchange and Reporting Portal that collects and distributes relevant cyber security information and alerts via text, email, RSS feeds and social media – targeting specific constituencies. Existing systems like the Innovate VA platform could likely be adapted for this use. Additionally, Virginia call center operators could screen reports of cyber incidents and requests for information to channel them to the appropriate response or assistance channel. The analysts, portal operators and call center staff could be co-located with the other Commonwealth, federal or private sector entities to provide a "unity of effort" approach, which would simplify communication and collaboration and enhance cyber security workforce development.

Commission Objectives 2015-2016

Working with the Virginia Cyber Security Commission, the work groups have developed the following objectives for 2015-2016.

Economic Development

The Economic Development Work Group will continue to collaborate with and assist the three public-private groups formed during 2014-2015 and will develop specific recommendations for consideration by the full Commission.

The Cyber Security for Advanced Manufacturing Group will continue to refine and formalize its initial recommendations. Applicable items will be forwarded to the full Commission for consideration.

The Automobile Cyber Security Group will complete a three-to-four month project to explore technology solutions for securing computer systems in automobiles. It will also develop approaches to scoring the cyber worthiness of vehicles.

The Cyber Security for Unmanned and Autonomous Aerial Vehicles Group will continue to develop strategies with the objective of establishing Virginia as the next innovation hub at the nexus of cyber security and unmanned systems by formally establishing a consortium focused on the issues related to cyber security and unmanned vehicles.

Education and Workforce

Based on the work completed during the 2014-2015, the Education and Workforce Work Group will focus on key ways education can build a vital and sustainable cyber security workforce.

Increase the pipeline of cyber security professionals by expanding articulation agreements between four-year colleges and community colleges – much as has been done between Northern Virginia Community College and George Mason University – to help community colleges prepare students to move into four-year cyber security programs or positions with industry. The work group will collaborate with the Governor's Virginia Community College System Office to determine actions and support needed to build regional relationships to generate guaranteed admission agreements. Specific recommendations and resources will be identified and submitted during the 2015-2016 legislative session.

Establish virtual access for small to mid-sized universities to cyber lab IT environments in larger schools and businesses. This access will give students hands-on experience in cyber defense operations and forensics and help smaller schools achieve designation as Centers for Academic Excellence in Information Assurance. Initial discussions with schools and industries housing these capabilities have been encouraging, and the work group will recommend action to enable cyber lab access for all schools.

Increase the number of faculty members with cyber security credentials. Faculty specifically trained and qualified to teach across the cyber curriculum are in high demand and very short supply, making it difficult for community colleges to attract and retain core faculty. Working with a broad range of stakeholders, the work group will develop strategies – such as endowed chairs, qualified industry professionals teaching courses and "virtual" professors shared among larger universities – to close the gaps.

Identify barriers that keep mid-sized universities and community colleges from developing accredited cyber programs quickly enough to keep pace with the accelerating need for cyber security professionals and create plans to overcome those roadblocks.

Review the results of the summer program at James Madison University to certify K-12 teachers in cyber security education and make further recommendations based on those results.

Cyber Crime Awareness

Over the course of the next year, the Cyber Crimes Awareness Work Group will continue ensuring that Virginia's laws remain current and in line with new technologies and statutes in other states, by following up on its recommendations to the Commission:

- Reintroduce an amendment to SB1189 for the authentication of Internet content via affidavit.
- Develop draft language to amend Virginia Code § 18.2-152.4 to set a lower standard of intent for computer trespass crimes.
- Work with the Commission to review and establish stricter penalties for computer crimes.
- Make recommendations to define 'protected' government computers and critical infrastructure systems and the penalties for intrusion into such systems.
- Work with the Commission to designate violations of the Virginia Computer Crimes Act as predicate offenses under the Virginia Racketeer Influenced and Corrupt Organization Act.
- Continue to investigate options for additional staff for the Virginia State Police, High Tech Crimes Division.

Additionally, the work group plans to further investigate Virginia's laws and regulations governing cyber crime so as to better protect its citizens and information systems.

Support civil suits against computer crimes. Virginia Code is not structured to support civil suits by owners of computer systems that were damaged by the types of offenses listed in the Virginia Computer Crimes Act. The work group will recommend that the Code be amended to allow such suits and to specify the types of relief that can be pursued.

Make it illegal to intentionally reveal three or more pieces of identifying information on the Internet. Under current Virginia law, it is not illegal to reveal someone else's identifying information on the Internet. The work group will advocate changing the statute to make the deliberate public posting of a combination of three pieces of such information on the Internet a misdemeanor.

Prohibit traffic in passwords or other means of access. Current statutory language may not provide sufficient tools to prosecute sellers or buyers of passwords and tools used to access computer systems. The work group will recommend that the Virginia Computer Crimes Act be updated to explicitly prohibit the sale or purchase of passwords, similar information or other means of access – regardless how the information was initially obtained.

Conduct additional evaluation for data breach legislation. As states and the federal government advance legislation governing prosecution of data breaches, the work group will recommend Virginia also seek clarification on the definitions, time frame for notifications and penalties related to these cyber crimes.

Cyber Infrastructure and Commonwealth Network Protection

Although the final analysis of the survey evaluating the cyber security posture of Virginia agencies is not yet complete, the work group expects to recommend actions, policy changes and key focus areas to ensure the Commonwealth's information technology assets are appropriately protected. Key recommendations being evaluated include:

- Identify and implement controls to reduce phishing attack vulnerabilities.
- Conduct a comprehensive inventory of cyber-physical systems in use.
- Conduct more frequent and robust sensitive-systems audits.
- Train and credential all agency information security officers.
- Evaluate risk profiles of Commonwealth systems currently operating on end-of-life software and develop remediation plans.
- Revamp privacy and data classification programs.
- Develop scenario-based cyber response playbooks to streamline response operations.

Similarly, the work group expects several high priority recommendations for safeguarding citizens' personally identifiable information to be developed based on the results of the initial PII survey, whose results had just been received while this report was in development.

Work on the identity and access management (IAM) effort begun in 2014-2015 will continue this year as the work group develops recommendations that ensure that all Commonwealth databases containing citizens' PII are encrypted and require multifactor authentication for access.

Evaluate creating a registry of volunteer certified security professionals willing to help localities and school districts with their cyber security capabilities could address the limited resources frequently preventing municipalities from acquiring the cyber security assistance they need – even with the National Guard helping assess and improve cyber readiness. The work group will also evaluate recommending some form of tax break for those who perform this type of pro bono work.

Public Awareness

The Public Awareness Work Group will continue to refine the requirements, capabilities and resources needed for the Cyber Information Exchange and Reporting Portal. This effort will be closely coordinated with Cyber Infrastructure and Commonwealth Network Protection Work Group activities related to the Joint Cyber Security Operations Center and the Virginia Information Sharing and Analysis Organization to ensure an integrated and cost effective approach to gathering, analyzing and disseminating cyber security information.

Based on the interest generated during the Virginia Cyber Security Commission's first year of cyber security outreach, the work group expects to continue conducting Town Hall meetings and other informational events throughout Virginia.

Appendix A

Executive Order 8

Commonwealth of Virginia Office of the Governor

Executive Order

NUMBER EIGHT (2014)

LAUNCHING "CYBER VIRGINIA" AND THE VIRGINIA CYBER SECURITY COMMISSION

Importance of the Issue

The Commonwealth of Virginia is proud of its distinguished history and exemplary record of exceptional cyber security operations in support of state agencies and operations. As is reflected in the strong presence of state, federal, military, and private cyber security businesses, assets, and activities throughout the Commonwealth, Virginia stands poised to take advantage of its unique resources. The Commonwealth is resolute in its dedication to garnering the expertise of leaders in cyber security in order to mitigate risks and safeguard the highest level of security for government infrastructure networks, foster cyber security education and awareness, incorporate innovative and best practices to protect data statewide, bolster business investment with public-private partnerships, and proactively enhance its national standing as one of the preeminent leaders in the cyber security arena.

Threats to critical systems present a growing and complex challenge. In order to guard against the risks and marshal appropriate resources to meet potential threats, it is important to incorporate optimal policies and develop enhanced standards to protect the Commonwealth's cyber security infrastructure from unforeseen incidents. While rapidly advancing technologies create substantial security risks, they also present significant opportunities for producing more efficient and protected proprietary networks, strengthening the Commonwealth's cyber security framework, and advancing vital prospects for economic development.

Virginia's cyber security businesses are at the forefront to prospectively benefit from federally appropriated funds that are among the few expected to increase in future years. Virginia's cyber security firms are seeking to export their technologies, goods and services to global markets in the public and private sectors. Further, with military assets, related defense activities and, more generally, the critical need for secure business data, the Commonwealth must cultivate conditions to attract and retain as well as secure a competitive advantage for cyber security companies in the marketplace. Promotion of the cyber security industry will produce a synergy to ensure growth of related cyber operations businesses and facilities, sustain a wide variety of high-skilled jobs for Virginians, and strengthen a culture of excellent cyber hygiene that is critical for the Commonwealth.

Cyber security instruction, training, and programs will be requisite components to prepare those currently seeking new occupational options as well as the next generation for the rapidly developing cyber security workplace. Focusing on cutting edge education and training will be essential for Virginia's cyber security workforce and economic development as occupations in the cyber security industry are highly in demand and among the fastest growing in the economy. Virginia continues to lead the nation in the concentration of technology workers, fed by a rich network of nationally-recognized information technology and cyber advanced degree programs at our universities.

Composition of the Commission

The Commission will consist of the Secretaries of Technology, Commerce and Trade, Public Safety, Education, Health and Human Resources, and Veterans Affairs and Homeland Security, and eleven (11) citizen members whose background shall include relevant expertise to be appointed by the Governor and serve at his pleasure. The Governor shall designate a Chairman and Vice Chairman from among the appointed members. The Governor may appoint additional persons to the Commission at his discretion.

Establishment of the Commission

Accordingly, by virtue of the authority vested in me as Governor under Article V of the Constitution of Virginia and under the laws of the Commonwealth, including but not limited to §§ 2.2-134 and 2.2-135 of the Code of Virginia, and subject to my continuing and ultimate authority and responsibility to act in such matters, I hereby establish the Virginia Cyber Security Commission.

Responsibilities of the Commission

Commission's responsibilities shall include the following:

1. Identify high risk cyber security issues facing the Commonwealth of Virginia.

2. Provide advice and recommendations related to securing Virginia's state networks, systems, and data, including interoperability, standardized plans and procedures, and evolving threats and best practices to prevent the unauthorized access, theft, alteration, and destruction of the Commonwealth's data.

3. Provide suggestions for the addition of cyber security to Virginia's Emergency Management and Disaster Response capabilities, including testing cyber security incident response scenarios, recovery and restoration plans, and coordination with the federal government - in consultation with the Virginia Information Technologies Agency.

4. Offer suggestions for promoting awareness of cyber hygiene among the Commonwealth's citizens, businesses and government entities.

5. Present recommendations for cutting edge science, technology, engineering and math (STEM) educational and training programs for all ages, including K-12, community colleges, universities, in order to foster an improved cyber security workforce pipeline and create cyber security professionals with a wide range of expertise.

6. Offer strategies to advance private sector cyber security economic development opportunities, including innovative technologies, research and development, and start-up firms, and maximize public-private partnerships throughout the Commonwealth.

7. Provide suggestions for coordinating the review of and assessing opportunities for cyber security private sector growth as it relates to military facilities and defense activities in Virginia.

Commission Staffing and Funding

Necessary staff support for the Commission's work during its continued existence shall be furnished by the Office of the Secretary of Technology, and such other agencies and offices as designated by the Governor. An estimated 500 hours of staff time will be required to support the work of the Commission.

Necessary funding to support the Commission and its staff shall be provided from federal funds, private funds, and state funds appropriated for the same purposes as the Commission, as authorized by § 2.2-135 of the Code of Virginia, as well as any other private sources of funding that may be identified. Estimated direct costs for this Commission are $5000.00.

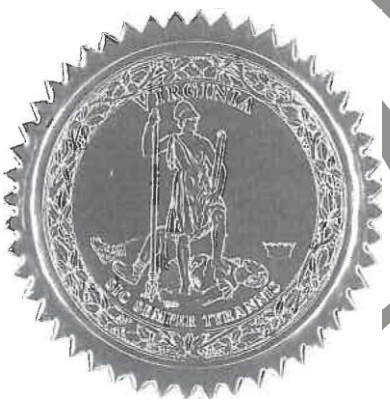
Commission members shall serve without compensation and shall receive reimbursement for expenses incurred in the discharge of their official duties.

The Commission shall serve in an advisory role, in accordance with § 2.2-2100 of the Code of Virginia and shall meet upon the call of the chairman at least three times per year. In addition, the Commission shall issue an annual report and any other reports and recommendations as necessary or as requested by the Governor.

Effective Date of the Executive Order

This Executive Order shall be effective upon its signing and shall remain in force and effect until February 25, 2015, unless amended or rescinded by further executive order.

Given under my hand and under the Seal of the Commonwealth of Virginia, this 25th day of February, 2014.



Terence R. McAuliffe, Governor

Attest: _____

Secretary of the Commonwealth

Appendix B

Virginia Cyber Security Commission Members

Commission is co-chaired by Richard Clarke and Secretary of Technology, Karen Jackson.

Richard A. Clarke, Chairman and CEO of Good Harbor Security Risk Management and an internationally recognized expert on cyber security, homeland security, national security, and counterterrorism. Mr. Clarke served the last three presidents as a Senior White House Advisor, including as Special Advisor to the President for Cyber Security and National Coordinator for Security and Counterterrorism, and was a member of President Obama's Review Group on Intelligence and Communication Technologies. He is a member of the Education and Workforce Work Group

Karen Jackson, Secretary of Technology and member of the Public Awareness Work Group.

Anne Holton, Secretary of Education and member of the Education and Workforce Work Group.

John Harvey, Secretary of Veterans and Defense Affairs and member of the Education and Workforce Work Group and the Economic Development Work Group.

Dr. Bill Hazel, Secretary of Health and Human Resources and member of the Infrastructure and Commonwealth Network Protection Work Group.

Maurice Jones, Secretary of Commerce and Trade and member of the Economic Development Work Group.

Brian Moran, Secretary of Public Safety and Homeland Security and member of the Cyber Crime Awareness Work Group.

Rhonda Eldridge, Director of Engineering at Technica Corp. where she leads six divisions within Technica and is responsible for internal research and development, visioning and business development – focusing on cutting edge cyber security and IT projects for federal customers including the Department of Defense. She is a member of the Public Awareness Work Group.

Jennifer Bisceglie, President and CEO of Interos Solutions, Inc. Ms. Bisceglie has more than 20 years of commercial technology and business operations experience in cyber security, business process re-engineering and commercial technology implementation for diverse companies industries and governments. She is chair of the Public Awareness Work Group.

Paul Kurtz, Chief Strategy Officer at CyberPoint. Mr. Kurtz leads the development and communication of CyberPoint's strategic vision for managing cyber threats. A recognized cyber security expert, he has held senior positions in both industry and government. During his government service, Kurtz was Special Assistant to the President and Senior Director for Critical Infrastructure Protection on the White House's Homeland Security Council. He is chair of the Infrastructure and Commonwealth Network Protection Work Group.

Paul Tiao, Attorney and partner with the international law firm of Hunton and Williams, LLP, where he is a leader in the firm's global privacy and cyber security practice. Prior to joining the firm, Mr. Tiao served as Senior Counselor for cyber security and technology to FBI Director Robert S. Mueller. He is chair of the Cyber Crime Awareness Work Group.

Barry Horowitz, Munster Professor of Systems and Information Engineering and Chair of the Systems and Information Engineering Department at the University of Virginia. Dr. Horowitz' research efforts center on economic models and system technologies related to cyber security. He currently is leading a Defense Department-sponsored research effort focused on embedding security solutions into systems, referred to as System Aware Cyber Security. Dr. Horowitz serves as a member of the Naval Studies Board of the National Academy of Science and recently led a Chief of Naval Operations-sponsored study for the board on cyber security. He is chair of the Economic Development Work Group.

Andrew H. Turner, Senior Vice President and Head of Global Security, VISA. Mr. Turner developed, from the ground up, VISA's Cyber Security organization, including the Attack Surface Management, Threat Intelligence, Incident Response and Digital Brand Protection Programs. He also implemented a Cyber Fusion-based program using intelligence collection, analysis and overall sensor enrichment to actively monitor and defend against global threats to the VISA enterprise and ecosystem. Prior to joining VISA, Mr. Turner served as Cyber Intelligence Practice Director for Microsoft Corp. He is chair of the Education and Workforce Work Group.

Jeffrey C. "J.C." Dodson, Global Chief Information Security Officer, BAE Systems. Mr. Dodson is a global cyber security expert across government, defense, aerospace, law enforcement and advanced technology sectors. He is the chairman of the Aerospace Industries Association's Industrial Security Committee and was appointed to serve as an Industry Representative to the federal government's National Industrial Security Program Policy Advisory Committee. He is a member of the Infrastructure and Commonwealth Network Protection Work Group and the Cyber Crime Awareness Work Group.

Jandria Alexander, Principal Director of the Cyber Security Subdivision in the Engineering Technology Group at the Aerospace Company. Ms. Alexander currently leads cyber and network security support to numerous customers and leads teams performing systems engineering for cyber operations, including architecture, requirements and concept of operations (CONOPS) support for integrating cyber operations into advanced ground and space segments. She is a member of the Economic Development Work Group and the Public Awareness Work Group.

Elizabeth "Betsy" Hight, Retired U.S. Navy Rear Admiral who served as the Vice Director of the Defense Intelligence Agency (DISA), Ms. Hight most recently served as Vice President of the Hewlett Packard's Enterprise Services U.S. Public Sector Cybersecurity Practice. She is a member of the Infrastructure and Commonwealth Network Protection Work Group.

John Wood, Chief Executive Officer, Chairman of the Board and Director for Telos Corp. As CEO, he orchestrates the company's support of the federal government in the critical areas of cyber operations and defense, secure communications and collaboration and identity assurance. He is a member of the Cyber Crime Awareness Work Group.

Rear Admiral Bob Day, U.S. Coast Guard (ret), Coast Guard CIO and Cyber Commander 2009-2014. He is the Virginia Cyber Security Commission Executive Director responsible for daily management of Commission activities.

Appendix C

Commission Meetings

The Commission and work groups conducted official meetings on the following dates:

June 11, 2014 - Inaugural Meeting
George Mason Inn, George Mason University

September 4, 2014 - Commission Meeting
Richmond Hilton Conference Center & Spa, Short Pump

November 7, 2014 - Commission Meeting
Patrick Henry Building, Richmond

March 18, 2015 - Commission Meeting
Patrick Henry Building, Richmond

May 6, 2015 - Commission Meeting
Virginia Tech Research Center, Arlington

July 7, 2015 - Commission Meeting
Patrick Henry Building, Richmond

Additional work group meetings were held on numerous dates.

All Commission and work group meeting agendas and minutes are available at https://cyberva.virginia.gov/Meeting-Resources.

Appendix D

Cyber Security-Related Legislation

There are 47 states, plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands that have notification requirements governing data breaches of personal information, according to the National Governors Association. Additionally, there are several bills in Congress addressing cyber security issues, most specifically data breaches. There are several common elements to this legislation:

Defining personal information, which usually consists of the consumer's name and other pieces of information that can range from Social Security or driver's license number to biometric data.

Requiring notification, which, in many states is within 30-45 days, although some state notification laws are triggered by the breach or when personal information was exfiltrated. Some states allow companies to evaluate the risk of misuse before determining whether notification is warranted.

Determining damages varies greatly among states, with some calculating penalties based on the number of consumers affected or the length of the notification delay. Many states have a maximum civil penalty for single breaches.

Designating an enforcing agency, which is usually the state attorney general.

Federal laws generally seek to preempt existing state statutes in an effort to apply a single standard for data breaches. The federal proposals usually allow state attorneys general to bring civil action on behalf of the state's residents to compel compliance with federal standards. In these provisions, the Federal Trade Commission has been given priority over the states in bringing action.

Federal Data Breach Legislation

H.R. 1770, Data Security and Breach Notification Act

The bill provides a national data security and breach notification standard in the event of identity theft or financial fraud. The bill defines what constitutes personal information and requires notification within 30 days of a breach in which more than 10,000 individuals were affected. The bill limits overall civil penalties for data breach notification to $2.5 million. The bill also preempts existing state data breach statutes "relating to or with respect to the security of data in electronic form or notification following a security breach of such data." The bill permits state attorneys general to bring civil action on behalf of the state's residents for additional compensation or to compel compliance with the federal standard; however, the Federal Trade Commission (FTC) retains primacy in civil prosecutions.

H.R. 580, Data Accountability and Trust Act

The bill requires the FTC to establish regulations for the protection of personal information held by the private sector and notification in case of a data breach. It also authorizes the FTC to conduct information security audits of companies that have experienced a security breach and requires companies holding individuals' personal information review it. The bill also includes requirements for the notification to affected individuals and sets maximum civil penalties for data breach notification of $5 million. The bill allows the enforcement of state consumer protection laws by state attorneys general and protects state trespass, tort and contract law or any other state law that relates to fraud. The bill permits state attorney's general to bring civil action on behalf of a state's residents for additional compensation or to compel compliance with the federal standard; however, the FTC retains primacy in civil prosecutions.

H.R. 1704, Personal Data Notification and Protection Act

The bill provides a national data security and breach notification standard and requires companies to provide notice to affected individuals within 30 days of discovering a breach that affects more than 10,000 individuals. The bill defines personal information and limits overall civil penalties for data breach notification to $1 million. Companies must also notify the major credit reporting agencies in case of a breach covered under the bill. The bill preempts state law "relating to notification by a business entity engaged in interstate commerce of a security breach…" The bill permits state attorneys general to bring civil action on behalf of the state's residents for additional compensation or to compel compliance with the federal standard; however, the FTC retains primacy in civil prosecutions.

H.R. 2205, Data Security Act

The bill is modeled on aspects of the Gramm-Leach-Bliley Act of 1999 and directs covered entities to develop an information security plan that requires them to: designate at least one employee to manage safeguards; conduct risk analyses; regularly assess the plan in light of risks; and update the program on a rolling basis as technology evolves. The bill also lays out clear requirements for consumer and law enforcement notification after a breach. The bill gives administrative enforcement authority to the regulatory agency under which the information would be applicable. Otherwise, enforcement authority resides with the FTC. The bill would preempt state authority related to data security protection and data breach notification requirements for private sector entities and individuals (also see S.961).

S. 177, Data Security and Breach Notification Act

The bill provides a national data security and breach notification standard in the event of identity theft or financial fraud. The proposal defines personal information and requires notification within 30 days to any individual whose personal data was reasonably believed to have been acquired. Federal law enforcement authorities must be notified within 60 days if more than 10,000 people were affected. Additionally, if more than 5,000 people were affected, then major credit reporting agencies must be notified. The bill sets maximum civil penalties for data breach notification of $5 million. The bill preempts existing state laws that govern private sector security practices or data breach notification with personal data. The bill allows the enforcement of state consumer protection laws by state attorneys general and also protects states laws that relate to fraud. The bill permits state attorneys general to bring civil action on behalf of a state's residents for additional compensation or to compel compliance with the federal standard; however, the FTC retains primacy in civil prosecutions.

S. 1027, Data Breach Notification and Punishing Cyber Criminals Act

The bill sets a national consumer-friendly data breach notification standard to protect and inform individuals when their personal information is compromised or made public. The bill also increases the maximum allowable fines and imprisonment for many of the most common cyber crimes. It requires consumers to receive notification within 30 days of discovery of data breaches with a description of information potentially accessed, how to inquire about what personal information was breached and how the information was unlawfully acquired. The bill also includes a new directive for diplomats at the State Department for apprehending and prosecuting cyber criminals in ongoing negotiations in countries that do not have an extradition agreement with the United States.

S. 961, Data Security Act

The bill requires an entity that determines sensitive information was (or may have been) compromised to investigate the scope of the breach and the type of information compromised and then determine whether the information will likely be used to commit identity theft or fraud. If it is determined that the information was compromised and will cause harm, then the entity must notify the appropriate federal government regulatory agency, law enforcement, national consumer reporting agencies (where the breach affects more than 5,000 consumers) and all consumers affected by the breach. The bill preempts state authority related to data security protection and data breach notification requirements for private sector entities and individuals (also see H.R. 2205).

S. 1158, The Consumer Privacy Protection Act

The bill requires companies that store sensitive personal or financial information on 10,000 customers or more to meet consumer privacy and data security standards to keep this information safe and to notify the customer within 30 days of a breach. It establishes a broad definition of information that must be protected and requires companies to inform federal law enforcement of all large breaches, as well as breaches that involved federal government databases or law enforcement or national security personnel. It preempts state laws "that are less stringent than the requirements of [the bill]," while leaving stronger state laws in place. The bill also prevents preemption of state laws or the enforcement of state laws related to consumer protection, trespass, contract, tort or acts of fraud.

Federal Information Sharing Legislation

H.R. 1731, National Cybersecurity Protection Advancement Act

The bill encourages the voluntary sharing of cyber threat information between the private sector and the federal government and directs the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) to share information with state, local and tribal governments. Measures would also need to be taken to remove personal information unrelated to a cyber risk or incident before sharing with the federal or non-federal government entities. Additionally, private companies would be provided with liability protection when sharing information through the NCCIC.

H.R. 1560, Protecting Cyber Networks Act

The bill allows the voluntary sharing of cyber threat information by the private sector and requires the Director of National Intelligence (DNI) to develop procedures to promote the sharing of cyber threat indicators from the federal government to private entities; non-federal government agencies; and state, local and tribal governments. The bill designates the newly created Cyber Threat Intelligence Integration Center (CTIIC) to manage the program and directs the CTIIC to analyze the cyber intelligence to inform the President, relevant agencies and Congress. Additionally, the bill imposes restrictions on the use, retention and search of any data voluntarily shared with the government and requires that personal information be removed from all shared information. Private companies would also be provided liability protection when sharing information.

H.R. 234, Cyber Intelligence Sharing and Protection Act

The bill directs the federal government to provide real-time sharing of cyber threat information between all designated federal cyber operations centers and appropriate national security agencies. The bill directs DHS, the Attorney General, the DNI and the Department of Defense (DOD) to establish procedures governing the receipt, retention, use and disclosure of non-publicly available cyber threat information shared with the federal government. Additionally, civil and criminal liability protections are provided to private companies sharing information with the federal government. The bill requires federal agencies receiving shared cyber threat information to facilitate collaboration with state, local, tribal and territorial governments.

S. 456, Cyber Threat Sharing Act

The bill permits the disclosure of cyber threat indicators to a private information sharing and analysis organization, which is to be established through a competitive process implemented by DHS and the NCCIC. It also allows private companies to receive indicators disclosed by federal, state and local governments. Private companies are granted liability protections when voluntarily sharing information with the NCCIC as long as those companies self-certify they have adopted best practices identified by DHS. It also directs DHS to designate the NCCIC to receive and disclose threat indicators to federal and non-federal entities in as close to real-time as possible.

S. 754, Cybersecurity Information Sharing Act

The bill requires the DNI, DHS, DOD and the Department of Justice to develop procedures that promote the timely sharing of cyber threat indicators with private companies, non-federal government agencies and state, tribal and local governments. The bill also provides liability protection to private companies that share cyber threat information. The bill permits state, tribal and local governments to use shared indicators (with the consent of the entity sharing the indicators) to prevent, investigate and prosecute cyber offenses.

S. 1023, Cybersecurity Information Sharing Credit Act

The bill gives businesses a tax credit for sharing information about cyber threats with other related businesses through a network of industry-specific groups called Information Sharing and Analysis Centers. The refundable credit allows businesses the opportunity to upgrade their online defenses and participate in an information sharing network without high upfront costs.

National Guard Role in Cyber Security Legislation

H.R. 60, Cyber Defense National Guard Act

The bill requires DNI to provide a report to Congress regarding the feasibility of establishing a Cyber Defense National Guard. The report must include analysis on a variety of issues related to potential cost, personnel, training, operations and logistics and include information on the number of people needed to defend the critical infrastructure of the United States from a cyber attack or man-made catastrophic incident; elements of the federal government that would be best equipped to recruit, train and manage such a National Guard; and the logistics of allowing governors to use such a National Guard in states during times of cyber emergency.

S. 1478, Department of Defense Cyber Support to Civil Authorities Act of 2015

The bill directs the Secretary of Defense to develop a comprehensive plan for the United States Cyber Command to support civil authorities in responding to cyber attacks by foreign powers. The plan must include steps to coordinate with state and local authorities.

Bill summaries are extracted from information provided by the National Governors Association.